Z Außen Sicherheitspolit (2016) 9:1–11
DOI 10.1007/s12399-015-0543-z

ANALYSE

Global Crime Governance: Perspektiven und Grenzen transnationaler Kooperation

Anja P. Jakobi · Jasmin Haunschild

Online publiziert: 16. Dezember 2015

Zusammenfassung Die Bekämpfung transnationaler Kriminalität ist ein wichtiger Teilbereich internationaler Politik, allerdings mit unklarer Erfolgsbilanz. Dieser Beitrag zeigt Möglichkeiten und Limitationen der grenzüberschreitenden Zusammenarbeit auf. So gehen erweiterte Kompetenzen staatlicher und nichtstaatlicher Akteure einher mit wenig Wissen um den Erfolg von Maßnahmen, divergierenden Interessen und Aufgaben, oder mangelnden Möglichkeiten, die Ursachen transnationaler Kriminalität zu bekämpfen. Anhand der Beispiele Menschenhandel/-schmuggel sowie Cyberkriminalität zeigen wir dabei auf, worin Schwierigkeiten der Einigung auf und der erfolgreichen Durchsetzung von effektiven Gegenmaßnahmen bestehen.

Schlüsselwörter Transnationale Kriminalität · *Global crime governance* · *Transnational governance* · Menschenhandel · Menschenschmuggel · Cyberkriminalität

Global Crime Governance: Perspectives and Limits of Transnational Cooperation

Abstract Global crime governance is an important part of international politics, yet its success remains questionable. This article analyses the possibilities and limits of transnational cooperation in this field. Extended mandates of state and non-state actors co-exist with divergent interests and aims, a lack of knowledge regarding

Dr. habil. A. P. Jakobi (✉) · J. Haunschild
Department of Politics and International Relations, Royal Holloway, University of London, TW20 0EX Egham, UK
E-Mail: a.p.jakobi@rhul.ac.uk

J. Haunschild
E-Mail: Jasmin.Haunschild@stud.tu-darmstadt.de

successful strategies, or lacking possibilities to counter many root causes of transnational crime. We use the examples of human smuggling/trafficking and cybercrime to illustrate specific difficulties of finding common ground and effective counter measures for fighting these crimes.

Keywords Transnational organized crime · Global crime governance · Transnational governance · Human trafficking · Human smuggling · Cybercrime

1 Einleitung

Die globale Bekämpfung von Kriminalität war lange ein Randbereich internationaler Politik, vorrangig der Zoll-oder Polizeizusammenarbeit überlassen, oder hauptsächlich im Rahmen des amerikanischen *war on drugs* (Andreas und Nadelmann 2006; Friesendorf 2007) thematisiert. Seit den 1990er Jahren hat sich jedoch ein tiefgreifender Wandel vollzogen, der sich teilweise durch einen größeren Problemdruck erklären lässt, teilweise jedoch auch durch ein geändertes Verständnis von Sicherheitspolitik und der *Versicherheitlichung* von ehemals eher peripheren Politikfeldern (Andreas und Price 2001).

Ein kurzer Blick in die Schlagzeilen der letzten Monate verdeutlicht, dass sehr unterschiedliche Phänomene mit dem Begriff *transnationale Kriminalität* in Verbindung gebracht werden – und dass die Grenzen zwischen kriminellen und nichtkriminellen Handlungen fließend sein können: So erfolgten durch US-Strafverfolgungsbehörden und unter Zuhilfenahme der Internationalen Kriminalpolizeilichen Organisation (Interpol) aufgrund vermuteter Korruption Ermittlungen gegen die in der Schweiz ansässige Fédération Internationale de Football Association (FIFA). Banken werden der internationalen Geldwäsche oder der Mithilfe zur Steuerhinterziehung verdächtigt. Die Diskussion um Flüchtlinge thematisiert oft den Menschenschmuggel, während das Ausspionieren des Computernetzwerks des Bundestages deutliche Hinweise auf das Sicherheitsrisiko durch Cyberkriminalität gibt.

Aus rechtspositivistischer Perspektive ist die Frage nach Kriminalität mit einem definierten Straftatbestand zu beantworten: Kriminell ist, was vom Gesetzgeber entsprechend definiert wird. Gleichzeitig spiegeln sich in der Gesetzgebung Pfadabhängigkeiten, Moralvorstellungen und – je nach Staat – auch religiöse Grundsätze. Die Flexibilität und Kontingenz dieser gesellschaftlichen Voraussetzungen führen einerseits zu veränderten Vorstellungen von Kriminalität, andererseits implizieren sie Schwierigkeiten für die internationale Kooperation.

Die entsprechende Konvention der Vereinten Nationen (United Nations Convention Against Transnational Organized Crime, UNTOC) definiert transnationale Kriminalität als eine in der Gruppe geplante oder durchgeführte Straftat mit grenzüberschreitender Planung oder Wirkung, die mit einer maximalen Freiheitsstrafe von mindestens vier Jahren geahndet werden kann. Zudem formuliert die Konvention noch bestimmte Straftaten – wie Korruption, Geldwäsche, Mitgliedschaft in einer kriminellen Vereinigung oder Justizbehinderung – die unabhängig von diesen Kriterien ihr Gegenstand sind (UNODC 2004). Während die Konvention einen wichtigen Meilenstein der internationalen Zusammenarbeit von Justiz und Strafver-

folgungsbehörden darstellt, basiert ein großer Teil internationaler Kooperation auf anderen Abkommen wie Rechtshilfeersuchen oder bilateraler Polizeizusammenarbeit. Daneben formulieren die UN einzelne Abkommen zum Drogenhandel oder zur Terrorismusfinanzierung. Ähnliche Aktivitäten sind auch in anderen internationalen Organisationen gängig, beispielsweise die Konvention der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) gegen Korruption, die EU-Direktiven zu Geldwäsche oder die Konvention des Europarates zu Cyberkriminalität. Die bestehenden multilateralen und bilateralen Aktivitäten sind allerdings häufig unzureichend, weshalb zunehmend andere *Governance*-Mechanismen entwickelt werden, mitunter unter Einbeziehung privater Akteure (Jakobi 2013; Jakobi und Wolf 2013; Jakobi 2015).

Im Folgenden werden wir einen kurzen Einblick in Mechanismen und Konflikte von g*lobal crime governance* geben. Daran anschließend werden die Aktivitäten von staatlichen und nichtstaatlichen Akteuren in der Verfolgung von transnationaler Kriminalität anhand von zwei aktuellen Diskussionen um Menschenhandel und -schmuggel sowie Cyberkriminalität erläutert. Im Ausblick werden Möglichkeiten und Grenzen von globaler Kriminalitätsbekämpfung kurz zusammengefasst.

2 Internationale Kooperation gegen transnationale Kriminalität

Die zwischenstaatliche Kooperation zur Bekämpfung von Kriminalität verzeichnet eine stetig höhere Regelungsdichte substantieller und prozeduraler Normen: Substantielle Normen definieren dabei eine immer größere Anzahl von Straftaten, denen durch internationale Kooperationen begegnet werden soll. Prozedurale Normen regeln die Art und Weise der Zusammenarbeit, beispielsweise die Kooperation von Behörden oder die Rückführung von durch Straftaten erlangten Gütern. Diese Regulierungsaktivitäten bedeuten jedoch nicht notwendigerweise eine effektive Unterbindung transnationaler Kriminalität, da dieser politikfeldspezifische Hindernisse, allgemeine Hindernisse der internationalen Kooperation und Probleme der weltweiten Implementierung entgegenstehen.

Ein zentrales *Governance*-Problem in diesem Politikfeld betrifft das eingeschränkte Wissen um das Ausmaß von Kriminalität, da kriminelle Aktivitäten sich bewusst der Öffentlichkeit entziehen. Schätzungen sind darum – mehr als in anderen Bereichen – Näherungswerte und Mutmaßungen über Dunkelziffern. Damit kann aber auch die Wirkung von *Governance*-Maßnahmen kaum bestimmt werden: So kann das Auffinden von mehr Schmuggelware an Grenzen bedeuten, dass insgesamt mehr geschmuggelt wird oder dass die Gegenmaßnahmen erfolgreicher sind und folglich mehr aufgedeckt wird. Effektivität von Kriminalitätsbekämpfung ist schon daher schwer zu bestimmen (Andreas und Greenhill 2010). Gleichzeitig steht die Politik unter großem Handlungsdruck, da die Öffentlichkeit Kriminalität in Umfragen oft als eines der größten sozialen Probleme nennt (Europäische Kommission 2011, S. 24). Diese Problemperzeption ist gleichzeitig nicht unbedingt abhängig von dem tatsächlichen Ausmaß der Kriminalität: So sinkt die Zahl vieler schwerer Straftaten, während dies auf die wahrgenommene Bedrohung durch Kriminalität kaum Einfluss zu haben scheint. Die Kombination von mangelnder Information bei gleich-

zeitigem Problemdruck gilt umso mehr im Hinblick auf transnational organisierte Kriminalität: Mit dem Ende des Kalten Krieges und der zunehmenden Integration der Weltwirtschaft und der globalen Finanzarchitektur sowie des Ausbaus der globalen Reise- und Transportmöglichkeiten wurden auch neue Möglichkeiten für kriminelle Aktivitäten geschaffen. Damit wurde Kriminalität verstärkt zu einem transnationalen Problem, weshalb sich die Anzahl der internationalen Regulierungsbemühungen seit den 1990er Jahren auch stark erhöht hat (Andreas und Nadelmann 2006; Jakobi 2013).

Die Etablierung und effektive Durchsetzung dieser internationalen Normen ist jedoch in mehrfacher Hinsicht voraussetzungsreich: Nötig ist zunächst ein gemeinsames Verständnis darüber, welche Handlungen kriminalisiert werden sollen und welche nicht. Trotz gemeinsamer Bekämpfungsziele auf nationaler und internationaler Ebene kann dabei sehr umstritten sein, was genau kriminalisiert und verfolgt werden soll. Weitere Hindernisse ergeben sich aus den unterschiedlichen Abläufen und Befugnissen kooperierender Stellen aufgrund verschiedener Organisationskulturen, aber auch unterschiedlicher Gesetzeslage: So ist der Umgang der Polizei mit der Bevölkerung sehr unterschiedlich, aber auch die Möglichkeiten der Ermittlung und der Beweisführung. Im Hinblick auf Cybercrime bedeutet dies beispielsweise, dass die Aufzeichnung, Speicherung und Auswertung elektronischer Daten in Großbritannien und den USA sehr viel einfacher ist als in Deutschland, was die entsprechenden Behörden mit mehr Wissen und Ermittlungsmöglichkeiten ausstattet – allerdings auf Kosten der Privatsphäre geht.

In ähnlicher Weise werden Banken auf die kontinuierliche Überwachung von Finanztransfers ihrer Kunden[1] verpflichtet, um damit Terrorismusfinanzierung oder Geldwäsche zu verhindern. Hier wurden seit 1989 umfangreiche, weltweite Regelungen eingeführt, die verschiedene Teile des Finanzsektors mit einer weitreichenden Informationspflicht belegen – wobei dieser sogar selbst seiner Rolle kritisch gegenüber steht (Bergström et al. 2011).

Eine aktivere Rolle nehmen private Akteure ein, wenn sie sich durch Selbstregulierung gleichzeitig an Normgenese und Implementation beteiligen, wie etwa bei der Unterbindung des Handels mit Konfliktdiamanten: 2003 trat das Kimberley Process Certification Scheme in Kraft, das sowohl Staaten zur Kontrolle und Transparenz der In- und Exporte von Rohdiamanten und zur Sicherung des Transports, als auch nichtstaatliche Akteure zur Selbstregulierung durch Zertifizierung verpflichtet (Jojarth 2009; Haufler 2009). Andererseits bleiben unabhängig von der Ausgestaltung der globalen Regelungen Umsetzungsprobleme bestehen, die aus schwer durchzuführenden Grenz- und Exportkontrollen, Korruption oder der möglichen Unterwanderung durch Marktteilnehmer resultieren. Auch daher kann die zunehmende Integration privater Akteure in *global crime governance* die Abhängigkeit von der Effektivität staatlicher Institutionen im Bereich Kriminalitätsbekämpfung nicht kompensieren.

[1] Im vorliegenden Artikel wird, abweichend vom ZfAS-Standard, bei personenbezogenen Substantiven die männliche grammatikalische Form verwendet. Die Autorinnen schließen damit Personen weiblichen wie männlichen Geschlechts gleichermaßen ein.

3 Maßnahmen gegen Menschenhandel und -schmuggel

Seitdem die Zahl von Flüchtlingen nach Europa in den letzten Monaten stark angestiegen ist, wird verstärkt über *Menschenschmuggel* und *Schleusen*, aber auch über *Menschenhandel* in den Medien berichtet. Menschenschmuggel und Schleusen wird in den internationalen Protokollen (als Teil der UNTOC) klar abgegrenzt von Menschenhandel, doch werden diese Aktivitäten in Realität und politischer Rhetorik oft zusammengebracht.

Beide Fälle sind üblicherweise mit einem illegalen Aufenthalt verbunden, Menschenhandel kann hingegen auch innerhalb von Landesgrenzen stattfinden. Die kriminelle Handlung im Fall von Menschenschmuggel ist primär die bezahlte Aktivität von Schleusern, durch Logistik oder gefälschte Papiere den illegalen Grenzübertritt zu ermöglichen. Menschenhandel dagegen steht im Zusammenhang mit der Ausbeutung der jeweiligen gehandelten Personen durch die Androhung oder Anwendung von Gewalt oder Zwang, durch Entführung oder Täuschung (UNODC 2004). Er wird größtenteils in Zusammenhang mit Zwangsprostitution diskutiert, obwohl er auch in anderen Sektoren stattfindet und dadurch erfolgen kann, dass zunächst geschleuste Menschen in extremen Formen von Schuldknechtschaft, in Zwangsarbeit oder Zwangsprostitution enden (UNODC 2014, S. 33–37). Umgekehrt ist nicht jeder Menschenschmuggler ein Menschenhändler. Oft wird das *Schleusen* oder *Schmuggeln* von den Migranten selbst eher mit einer Dienstleistung in Verbindung gebracht als mit einer kriminellen Handlung. Entsprechend unterschiedlich sind die Geschädigten: Im Fall von Menschenhandel werden primär die Menschenrechte eines gehandelten Menschen missachtet, im Fall von Menschenschmuggel die jeweiligen nationalen Einreise- und Aufenthaltsregelungen. Allerdings missachten auch Menschenschmuggler – wie vielfach an Todesfällen zu beobachten – die Menschenrechte der Geschleusten. Diese Gefährdung wird von diesen jedoch mangels alternativer Einreisemöglichkeiten in Kauf genommen.

Bis zu der Diskussion um Menschenschmuggel und die deutlich gewachsene Anzahl an Migranten und Asylbewerbern stand Menschenhandel im Zentrum der politischen Aufmerksamkeit. Hier sind zivilgesellschaftliche Organisationen stark engagiert, primär um Aufmerksamkeit und Unterstützung für die Opfer von Menschenhandel zu gewinnen. So wurden schon seit Beginn des 20. Jahrhunderts, vor allem mit Blick auf Prostitution und infolge eines gestärkten Menschenrechtsdiskurses, globale Regime zur Bekämpfung von Menschenhandel vorangetrieben, sodass heute UN-Protokolle und eine Vielzahl nationaler und internationaler Regelungen gegen diesen Straftatbestand existieren.

Die Verfolgung von Menschenhandel und -schmuggel wird allerdings dadurch erschwert, dass teilweise widersprüchliche Ansätze verwirklicht werden: So besteht seit langem eine unversöhnliche Diskussion darüber, wie das Verhältnis von Prostitution und Menschenhandel zu definieren sei. Hier reiben sich unterschiedliche Staaten

und vor allem zivilgesellschaftliche Organisationen daran auf, ob Prostitution und Menschenhandel stets gleichzusetzen sind (und damit Prostitution immer zu kriminalisieren ist) oder ob letzteres eine Straftat und ersteres eine Dienstleistung darstellt (und Prostitution damit zu entkriminalisieren ist). Die Intensität der Debatte hat die globale Regulierung von Menschenhandel und Menschenschmuggel jedoch kaum voran gebracht; im Gegenteil hat sie dazu geführt, dass dieser Bereich global und in den meisten Staaten vorrangig mit Hinweis auf Kriminalität diskutiert wird und weniger in Bezug auf die Menschenrechtsverletzungen, die damit einhergehen.

Der Kontrast zwischen strafverfolgungsorientierten und menschenrechtsorientierten Perspektiven ist aktuell nicht nur in Bezug auf Opfer des Menschenhandels, sondern auch von -schmuggel stark hervorgetreten: Während einerseits polizeiliche und auch militärische Maßnahmen gegen Schleusungen erwogen werden und damit die Diskussion um Kriminalitätsbekämpfung kreist, gibt es zudem, aufgrund steigender Todesfälle in Zusammenhang mit Bootsunglücken, eine zunehmende Anerkennung der illegalen Migranten als Opfer von Menschenrechtsverletzungen. Bis vor kurzem wurden bei Debatten über illegale Migration eher die *Schleuser* in den Mittelpunkt gerückt, beispielsweise in Diskussionen um die Zerstörung von Schleuserbooten vor der libyschen Küste (FAZ 2015). Diese Verweise auf geplante oder durchzuführende Kriminalitätsbekämpfung sind sachlich jedoch nur begrenzt hilfreich, da diese Schleuserboote oft erst als solche zu erkennen sind, wenn sie sich bereits mit Passagieren auf See befinden. An anderen Stellen wiederum – so bei der Passage von der Türkei nach Griechenland – werden eher Schlauchboote eingesetzt, die einfach und unauffällig zur Küste zu transportieren sind.

Doch selbst effektivere Kriminalitätsbekämpfung kann die Probleme illegaler Migration kaum lösen. Die Asymmetrie von Lebensbedingungen bei gleichzeitig gestiegenen Kommunikations-, Reise- und Transportmöglichkeiten bedeutet für potentielle Migranten aus Kriegs- und Krisengebieten langfristig einen einfacheren Zugang zu ehemals kaum erreichbaren Staaten. Diskussionen um Menschenschmuggel und die Aufdeckung krimineller Schmugglernetzwerke können zwar dazu beitragen, dass Migrationsprozesse weniger gefährlich werden – solange aber gefährliche Schmugglermethoden von Migranten in Krisengebieten noch als eine Hilfeleistung wahrgenommen werden, sind die Erfolge in der Bekämpfung von Menschenschmugglern absehbar begrenzt. Besonders die Flexibilität organisierter krimineller Netzwerke und die unelastische Nachfrage nach Schleusungen deutet darauf hin, dass solche Maßnahmen vornehmlich zu einer Änderung der Schmuggelrouten führen und durch ein verknapptes Angebot zu einer weiterhin steigenden Gewinnmarge für Schleuser und zu noch gefährlicheren Transporten führen würde – beides scheint sich durch vermehrte Nachrichten über zu Tode gekommene Flüchtlinge auf den Landrouten zu bestätigen (Die Welt 2015).

Die Regulierung legaler Migration kann sich auf Menschenhandel und -schmuggel auswirken, allerdings ist die Wirkung nicht eindeutig belegt. Die bestehenden UN-Protokolle sind jedoch keine *Governance*-Instrumente zur Regulierung von illegaler Migration, sondern eher Ausdruck dessen, dass Menschenhandel und Menschenschmuggel normativ nicht erwünscht sind. Allerdings bleibt bisher unklar, wie effektive Instrumente in diesen Bereichen aussehen, da jegliche Maßnahmen auch gegenteilige Folgen haben können. Im Hinblick auf Menschenhandel deutet einiges

darauf hin, dass die Nachfrage nach billigen Arbeitskräften unelastisch ist und Menschenhandel diese Nachfrage in unterschiedlichen Sektoren bedient. Dann läge eine Lösung in dem Verbot und der Verfolgung bestimmter Arbeitsverhältnisse, mit dem Ziel, diese zu unterbinden. Allerdings ist es auch möglich, dass beispielsweise gerade die Kriminalisierung von Prostitution zu erhöhten Gewinnen für kriminelle Gruppen führen kann, wodurch der Handel mit Menschen für sie lukrativer wird (Akee et al. 2014; Avdan 2012).

Menschenschmuggel kann wiederum begegnet werden, indem Grenzübertritte generell erschwert werden. Dies ist aber unter der Maßgabe offener Grenzen oft weder möglich noch politisch gewünscht. Mehr noch bedient dies letztendlich den Markt der Schleuser, da diese gerade dadurch nachgefragt und Transporte besonders gefährlich werden.

4 Maßnahmen gegen Cyberkriminalität

Der verbreitete Einsatz von Computern hat nicht nur die Begehung bekannter Straftaten vereinfacht, sondern auch ganz neue – legale wie illegale – Betätigungsfelder geschaffen. Aufgrund der sich ständig wandelnden technologischen Möglichkeiten, konfligierender staatlicher Interessen, der Anpassungsfähigkeit von *hacking codes* sowie der territorialen Ungebundenheit von Hackern gestalten sich eine globale Regulierung und deren effektive Durchsetzung schwierig. Zusätzlich bestehen kaum Erfahrungen in der Regulierung eines virtuellen Politikbereiches, bei dem traditionelle Vorstellungen von Territorialität schwer aufrecht zu halten sind.

Bei Cyberkriminalität kann zunächst zwischen Cybercrime und *cyberwar* unterschieden werden. Dabei umfasst Cybercrime kriminelle Aktivitäten, die z. B. durch Identitätsdiebstahl und Betrug primär ökonomischen Schaden an privaten Unternehmen und Einzelpersonen anrichten. *Cyberwar* dagegen bezeichnet Angriffe auf kritische Infrastruktur von Energieversorgern zu Militärinstitutionen, in deren Konsequenz der gesellschaftliche und wirtschaftliche Alltag eines Landes bedeutend eingeschränkt werden kann, auch mit militärischen Zielen wie der Schwächung von Organisationsfähigkeit. Die Abgrenzung von öffentlichem und privatwirtschaftlichem Ziel des *cyberwar* ist schwierig, da auch private Unternehmen essentiell für die öffentliche Sicherheit sein können, wenn sie öffentliche Infrastruktur und Güter bereitstellen.

Es scheint sinnvoll, grundsätzlich Opfer, Täter und Schadensart von Cyberkriminalität zu unterscheiden. Hier zeigt sich ein komplexes Bild, da Staaten Opfer von Cyberattacken werden, aber auch andere Staaten angreifen und ihre Bürger unrechtmäßig überwachen können. Andererseits können Hacker öffentliche Infrastruktur schädigen oder auf bestehende Sicherheitslücken aufmerksam machen und den Nutzern unbekannte Überwachung aufzeigen (Kühl 2015). Aber auch ein Blick auf die Wahrscheinlichkeit bestimmter Angriffe zeigt, dass hier – wie bei Risikopolitik üblich (Daase 2002) – potentiell große Gefahren, deren Eintreten sehr unwahrscheinlich ist, mehr Aufmerksamkeit erfahren als häufiger auftretende Angriffe mit weniger Gefahrenpotential. Die oftmals sehr abstrakt wirkende Bedrohungslage und die Unschärfe der Begriffe rund um kriminelles Verhalten im Cyberspace lässt sich

dabei politisch ausnutzen. Es macht aber auch den dort befürchteten oder entstandenen Schaden schwer abschätzbar, zumal viele Untersuchungen von Cyberkriminalität durch in diesem Feld aktive Unternehmen durchgeführt werden (Anderson et al. 2013, S. 267).

Während häufig das Bild entsteht, dass die Politik gänzlich den Regeln und Neuerungen des Cyberspace unterlegen sei, zeigt sich die Regulierungsgewalt des Staates doch durchaus auch in dieser Sphäre, etwa an Online-Zensur, Datenspeicherungsvorgaben oder dem Zwang, Software so zu programmieren, dass sie von Geheimdiensten besser überwacht werden kann (Deibert und Crete-Nishihata 2012). Bei nationalstaatlicher Regulation bleibt allerdings das Problem bestehen, dass sowohl Programmierer als auch Hacker dadurch, dass sie kaum Infrastruktur benötigen, territorial wenig gebunden sind und in weniger streng regulierende Staaten ausweichen können.

Dieser Hintergrund macht die Unterschiede zwischen einzelnen Ländern besonders problematisch und die Notwendigkeit einer umfassenden, globalen Regulierung sichtbar. Allerdings stehen dieser erhebliche Kooperationshindernisse gegenüber: insbesondere die Wahrung staatlicher Souveränität, Sorgen um die nationale Sicherheit, sozio-kulturelle Unterschiede im Hinblick auf Kriminalisierung, sowie Implementierungschwächen.

Während jegliche globale Regulierung von Kriminalität in Nationalstaaten politisch sensibel sein kann, da Strafrechts- und Polizeiprozesse Kernthemen staatlicher Souveränität ausmachen, wird dies im Falle von Cyberkriminalität durch den Nexus zu *cyberwar* noch verstärkt. Wenn globale Regime zur Kontrolle von Cyberkriminalität nicht effektiv durchgesetzt werden, schränken sich diejenigen Staaten mehr ein, die die Regelung durchsetzen und erhalten relative Nachteile im Vergleich zu jenen, die sich nicht konform verhalten. Dies betrifft insbesondere die Nutzung offensiver Techniken wie sie in Szenarien von *cyberwar* oft diskutiert werden. Eine globale Definition und Regulierung von Cyberkriminalität würde die Fähigkeiten von Armeen oder Geheimdiensten zwar zunächst nicht einschränken, könnte diese jedoch langfristig stärker begründungsbedürftig machen und damit Regulierungsbedarf einleiten (ähnlich den Abkommen in Bezug auf andere Waffensysteme).

Zudem spielen besonders bei der Kriminalisierung von Taten sozio-kulturell geprägte Ansichten eine große Rolle (Kshetri 2013). Eine starke Konfliktlinie innerhalb der Staaten ist außerdem die Abwägung von Sicherheit durch vereinfachte Überwachung und Datensammlung im Gegensatz zur Wahrung der Privatsphäre. Dies betrifft nicht nur die Ausbalancierung in Demokratien, sondern auch die Frage, inwieweit eine globale Regulierung letztendlich autoritären Regimen dienen kann, die ein besonders großes Interesse an verstärkten Möglichkeiten der Überwachung haben. Zu den politischen Herausforderungen kommen technische Umsetzungsschwierigkeiten, besonders durch schnellen technologischen Wandel. Da zukünftige Änderungen schwer vorhersehbar sind, muss ein Regime Flexibilität erlauben, um anpassungsfähig zu bleiben, was gegen einen hohen Grad an Legalisierung spricht (Abbott et al. 2000). Andererseits wird den zuvor beschriebenen Sicherheitserwägungen ein hoher Grad an Legalisierung durch hohe Verbindlichkeit eher gerecht.

Dies erklärt zum Teil, warum bisher kein globales Regime existiert. Die einzige bedeutende Konvention ist die des Europarates, die 2001 angenommen und bisher

von 50 Staaten, darunter auch Nicht-EU-Staaten, ratifiziert wurde (Council of Europe 2015). Diese kriminalisiert unter anderem Betrug, Kinderpornografie, unerlaubten Zugang zu Netzwerken (Council of Europe 2001) sowie durch ein Zusatzprotokoll inhaltsbezogene Straftaten wie *hate speech*. Schon hier zeigen sich Konfliktlinien, die auch bei der aktuellen Debatte um Hetzreden auf Facebook deutlich werden: Das Protokoll zu *hate speech* wurde aus der Konvention ausgegliedert, weil es amerikanische Prinzipien der freien Rede stark einschränken würde. Die virtuelle Kommunikation auf der gleichen sozialen Medienplattform wird je nach Staat unterschiedlich reguliert. Dies ist nicht nur technisch schwierig, sondern lässt sich oft durch geschickte Nutzer umgehen. In der Konsequenz sind hier globale, weniger territorial gebundene Ansätze nötig, gleichzeitig aber bisher kaum realisierbar. Schon innerhalb Europas sind Direktiven zu Cyberkriminalität nicht unproblematisch, da sie einige Länder besonders im Bereich Datenspeicherung ausbauen möchten, während angestrebte Regelungen in anderen, wie Deutschland, gegen das Grundgesetz verstoßen (BBC 2014).

Durch die divergierenden Interessen und Ansätze findet Kooperation oft auf bilateraler Ebene statt – auch angeschlossen an bestehende Institutionen wie Interpol (Choucri et al. 2014) – und fokussiert auf Straftaten, die länderübergreifend als besonders gravierend wahrgenommen werden. Trotz der Hindernisse ist daher z. B. das Auffinden von Kinderpornografie ein Beispiel für erfolgreiche Kooperation, und vielfach haben hier Polizeibehörden, Internetanbieter und Zahlungsdienstleister international zusammengearbeitet und entsprechende Netzwerke aufgedeckt. Auch ist davon auszugehen, dass Geheimdienste kooperieren und große Teile des Cyberspace effektiv überwachen können; dies entzieht sich jedoch in weiten Teilen der Öffentlichkeit.

Es handelt sich um ein Politikfeld, in dem vorrangig technische Fragen diskutiert werden und verhältnismäßig wenig zivilgesellschaftliches Engagement zu sehen ist. Als erster größerer Schritt einer globalen Öffentlichkeit hat sich eine Koalition von Nichtregierungsorganisationen (NGOs) zusammengefunden, die für die Wahrung individueller Rechte im Internet eintritt: die Internet Rights and Principles Coalition (2014). Es ist jedoch offen, ob dies langfristig ein gestiegenes Interesse der Zivilgesellschaft signalisiert. Die Einbindung privater Akteure betrifft bisher eher die Implementierung staatlicher Vorgaben, insbesondere aufgrund der technischen Komplexität und der tragenden Rolle von Internetdienstleistern und Softwarefirmen: Auf nationaler Ebene werden beispielsweise an Internet- und Kommunikationsanbieter Datensicherungsaufgaben delegiert. Diese können auch dazu verpflichtet werden, Verbindungs- und Kommunikationsdaten herauszugeben (Deibert und Rohozinski 2010). Allerdings sind in Reaktion darauf viele bedeutende Internetdienstleister dazu übergegangen, in *transparency reports* zu berichten, welche Art von Anfragen sie von staatlicher Stelle bezüglich der Herausgabe von Daten oder dem Löschen von Inhalten bekommen, mit welchen Begründungen und in welchen Fällen sie ihnen stattgegeben haben. Viele haben sich zudem *guidelines for law enforcement* gegeben und sich darin unter anderem auferlegt, betroffene Nutzer über die staatlichen Anfragen zu informieren (Twitter 2015).

Die Bekämpfung von Cyberkriminalität zeigt beispielhaft, wie sehr sich Kriminalität und deren Verfolgung grundsätzlich wandeln – im Hinblick auf die Vielzahl der

öffentlichen und privaten Täter und Verfolger, aber auch im Hinblick auf mehr Streitfragen darüber, was als eigentliche, kriminelle Handlung zu verstehen ist.

5 Schlussfolgerungen und Ausblick

Transnationale Kooperation gegen Kriminalität hat sich in den letzten Jahren stark verändert, ebenso wie die Herausforderungen, auf die sie reagiert. Wie groß der Abschreckungs- und Aufklärungseffekt von *global crime governance* letztendlich ist, lässt sich aufgrund mangelnder Daten kaum abschätzen. Allerdings kann im Umkehrschluss gelten, dass Kriminalität ohne Eindämmungsversuche wesentlich weiter verbreitet wäre. Selbst die Signalwirkung von weniger effektiven Maßnahmen ist daher nicht zu unterschätzen, wenngleich sie wiederum eine Symbolpolitik begünstigen kann.

Insgesamt kann erwartet werden, dass dieser Bereich weiterhin ein expandierender Teil internationaler Politik bleibt. Zu den Kooperationen in diesem Bereich kommt ein größeres öffentliches Bewusstsein für Probleme mit Kriminalität in anderen Ländern hinzu, ebenso wie die zunehmende Extraterritorialität der Kriminalitätsbekämpfung, die ein globales Verständnis des Problembereiches fördert. Während in diesem Beitrag vielfach die Hindernisse erfolgreicher Kooperation angeführt wurden, sollte daher auch nicht aus dem Blick geraten, dass durch die hohe Anzahl substantieller und prozeduraler Normen, genau wie durch die Einbindung privater Akteure, die Möglichkeiten der Kriminalitätsbekämpfung erweitert wurden.

Literatur

Abbott, K. W., Keohane, R. O., Moravcsik, A., Slaughter, A., & Snidal, D. (2000). The concept of legalization. *International Organization, 54*(3), 401–419.

Akee, R., Basu, A., Bedi, A., & Chau, N. H. (2014). Transnational trafficking, law enforcement, and victim protection: A middleman trafficker's perspective. *Journal of Law and Economics, 57*(2), 349–386.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Hrsg.), *The economics of information security and privacy* (S. 265–300). Berlin, Heidelberg: Springer.

Andreas, P., & Greenhill, K. M. (Hrsg.). (2010). *Sex, drugs and body counts. The politics of numbers in global crime and conflict*. Ithaca: Cornell University Press.

Andreas, P., & Nadelmann, E. (2006). *Policing the globe. Criminalization and crime control in international relations*. Oxford: Oxford University Press.

Andreas, P., & Price, R. (2001). From war fighting to crime fighting: Transforming the American national security state. *International Studies Review, 3*(3), 31–52.

Avdan, N. (2012). Human trafficking and migration control policy: Vicious or virtuous cycle? *Journal of Public Policy, 32*(3), 171–205.

BBC. (2014, 8. Apr.). Top EU court rejects EU-wide data retention law. http://www.bbc.co.uk/news/world-europe-26935096. Zugegriffen: 25. Sep. 2015.

Bergström, M., Helgesson, K. S., & Mörth, U. (2011). A new role for for-profit actors? The case of anti-money laundering and risk management. *Journal of Common Market Studies, 49*(5), 1043–1064.

Choucri, N., Madnick, S., & Ferweda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development, 20*(2), 96–121.
Council of Europe. (2001). Convention on cybercrime. Explanatory report. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm. Zugegriffen: 25. Sep. 2015.
Council of Europe. (2015). Convention on cybercrime. Status as of 1/1/2015. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG. Zugegriffen: 25. Sep. 2015.
Daase, C. (2002). Internationale Risikopolitik. Ein Forschungsprogramm für den sicherheitspolitischen Paradigmenwechsel. In C. Daase, S. Feske, & I. Peters (Hrsg.), *Internationale Risikopolitik. Der Umgang mit neuen Gefahren in den internationalen Beziehungen* (S. 9–35). Baden-Baden: Nomos.
Deibert, R., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance: A Review of Multilateralism and International Organizations, 18*(3), 339–361.
Deibert, R., & Rohozinski, R. (2010). Under cover of the net: The hidden governance mechanisms of cyberspace. In A. L. Clunan, & H. A. Trinkunas (Hrsg.), *Ungoverned spaces: Alternatives to state authority in an era of softened sovereignty* (S. 255–272). Stanford: Stanford University Press.
Die Welt. (2015, 28. Aug.). 71 Leichen aus Lkw geborgen – drei Festnahmen. http://www.welt.de/politik/ausland/article145730535/71-Leichen-aus-Lkw-geborgen-drei-Festnahmen.html. Zugegriffen: 20. Sep. 2015.
Europäische Kommission. (2011). Standard-Eurobarometer 75. http://ec.europa.eu/public_opinion/archives/eb/eb75/eb75_publ_de.pdf. Zugegriffen: 20. Sep. 2015.
FAZ.net. (2015, 18. Mai). EU-Beratungen: Militär soll Schlepperboote im Mittelmeer zerstören. http://www.faz.net/aktuell/politik/europaeische-union/eu-will-fluechtlings-schlepperboote-im-mittelmeer-versenken-13598664.html. Zugegriffen: 20. Sep. 2015.
Friesendorf, C. (2007). *US foreign policy and the war on drugs. Displacing the cocaine and heroin industry*. London: Routledge.
Haufler, V. (2009). The Kimberley process certification scheme: An innovation in global governance and conflict prevention. *Journal of Business Ethics, 89*(4), 403–416.
Internet Rights and Principles Coalition. (2014). The charter of human rights and principles in the internet. http://internetrightsandprinciples.org/site/charter/. Zugegriffen: 25. Sep. 2015.
Jakobi, A. P. (2013). *Common goods and evils? The formation of global crime governance*. Oxford: Oxford University Press.
Jakobi, A. P. (2015). Non-state actors and global crime governance: Explaining the variance of public-private interaction. *The British Journal of Politics & International Relations*. http://onlinelibrary.wiley.com/doi/10.1111/1467-856X.12064/pdf. Zugegriffen: 20. Sep. 2015.
Jakobi, A. P., & Wolf, K. D. (Hrsg.). (2013). *The transnational governance of violence and crime: Non-state actors in security*. Houndsmill: Palgrave Macmillan.
Jojarth, C. (2009). *Crime, war and global trafficking. Designing international cooperation Cambridge*. Cambridge: Cambridge University Press.
Kshetri, N. (2013). Cybercrime in the former Soviet Union and Central and Eastern Europe: Current status and key drivers. *Crime, Law and Social Change, 60*(1), 39–65.
Kühl, E. (2015, 7. Juli). Dubiose Deals und Teure Trojaner. Zeit Online. http://www.zeit.de/digital/datenschutz/2015-07/hacking-team-trojaner-kunden-hack. Zugegriffen: 20. Sep. 2015.
Twitter. (2015). Richtlinien für Strafverfolgungsbehörden. https://support.twitter.com/articles/20170305. Zugegriffen: 20. Sep. 2015.
UNODC – United Nations Office on Drugs and Crime. (2004). United Nations convention against transnational organized crime and the protocols thereto. http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf. Zugegriffen: 1. Sep. 2015.
UNODC. (2014). *Global report on trafficking in persons*. Wien: UNODC.